Joshua B. Swigart (SBN 225557)
Josh@SwigartLawGroup.com
Swigart Law Group, APC
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
P: 866-219-3343
F: 866-219-8344

Ben Travis
ben@bentravislaw.com
Ben Travis Law, APC
4660 La Jolla Village Drive, Suite 100
San Diego, CA 92122
Phone: (619) 353-7966

Attorneys for Plaintiff and The Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of others similarly situated, Plaintiff, vs. TALKIATRY MANAGEMENT SERVICES, LLC, Defendant.	Case No: _____ CLASS ACTION **COMPLAINT FOR DAMAGES:** 1. **Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)** 2. **Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631** 3. **Invasion of Privacy Under California's Constitution** 4. **Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code. § 502**

	5. Use of a Pen Register or Trap and Trace Device, Cal. Penal Code § 638.51 **6. Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030** **7. Violation of the Stored Communications Act, 18 U.S.C. § 2701** **Jury Trial Demanded**

INTRODUCTION

Plaintiff Jane Doe ("Plaintiff") brings this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Defendant Talkiatry Management Services, LLC ("Talkiatry" or "Defendant"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendant for disclosing confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to Meta Platforms, Inc. ("Meta"), via a tracking pixel ("Meta Pixel") in violation of various common and statutory data privacy laws.

2. Defendant maintains the website: https://www.talkiatry.com/ (the "Website"), which allows consumers to find information about various mental health conditions and what kinds of treatments are available. It also allows visitors to sign up and receive virtual mental health care.

3. When engaging with Defendant's online resources, safeguarding personal health information is paramount. Users anticipate that their data will remain confidential and not be disclosed to third parties without explicit consent. This expectation is particularly significant when accessing sensitive health topics, such as mental health.

Interactions on these subjects may involve deeply personal details, including medical histories and personal experiences, as well as searches involving sensitive medical subjects. The emotionally sensitive and potentially stigmatizing nature of this information underscores the critical importance of robust data protection measures to maintain user trust and ensure privacy.

4. Moreover, information concerning an individual's healthcare, including mental health, is protected by state and federal law.

5. Despite these protections, and unbeknownst to Plaintiff and Class Members, Defendant shares Website visitors' personal information with Meta using a "Meta Pixel" which is a snippet of programming code that, once installed on a webpage, sends information to Meta.

6. The Meta Pixel sends information to Meta in a data packet containing PII, which Meta then stores on its own servers.

7. The information that Defendant shares with Meta includes the consumer's unique Facebook ID ("FID") and the pages that the person visited, among other information. A consumer's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the consumer.

8. Defendant discloses the consumer's FID and page visits to Meta together in a single transmission. Because the FID uniquely identifies an individual's Facebook account, Meta, as well as any other person, can use the FID to quickly and easily locate, access, and view that person's corresponding Facebook profile. In simplest terms, the

Meta Pixel allows Meta to know what mental health conditions one of its members viewed on Defendant's website.

9. The Private Information that Defendant discloses through the Meta Pixel is valuable to internet marketing companies like Meta as they receive, view, analyze, and aggregate the information to build consumer profiles to assist advertisers in targeting desired demographics.

10. Plaintiff brings this action for legal and equitable remedies resulting from these illegal actions.

PARTIES

11. Plaintiff Jane Doe is a natural person and an adult citizen of the state of California, domiciled in Rancho Cucamonga, California.

12. Defendant is a limited liability company formed in New York with its principal place of business located at 109 W 27th St, Suite 5S, New York, NY, 10001. Defendant operates, amongst other things, the Website, that is the subject of this litigation.

Jurisdiction And Venue

13. Jurisdiction of this Court is proper pursuant to 28 U.S.C. § 1331 because this action arises out of Defendant's violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2510 et seq.

14. This Court also has federal subject matter jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a proposed class

action in which there are at least 100 Class members, the amount in controversy exceeds $5,000,000, and Defendant and Plaintiff are diverse.

15. Plaintiff is requesting statutory damages of $10,000 per violation of the ECPA, which when aggregated among a proposed class number in the thousands, far exceeds the $5,000,000 threshold for federal court jurisdiction under CAFA.

16. Therefore, this Court has federal subject matter jurisdiction.

17. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in California. The violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of California, such as Plaintiff, while they were located within California. At all relevant times, Defendant did business over the internet with residents of California, including Plaintiff. Defendant knew that its practices would directly result in real-time viewing and collection of information from California citizens while those citizens were engaged in commercial activity on Defendant's website. Defendant also maintains psychiatrists in California. Defendant chose to benefit from marketing and doing business in California. The claims alleged herein arise from those activities.

18. Defendant also conducts business within the State of California by maintaining an address at 100 Pine St, Suite 1250, San Francisco, CA 94111 from where its psychiatrists provide services.

19. Venue is proper pursuant to 28 U.S.C. § 1391 for the following reasons:

(i) the conduct complained of herein occurred within this judicial district; and (ii) Defendant conducted business within this judicial district at all times relevant.

FACTUAL ALLEGATIONS

A. COMMON ALLEGATIONS

20. Defendant's Website allows visitors to seek out information about various mental health conditions including potential treatments. It also allows visitors to sign up and match with psychiatrists who can evaluate them and provide them with recommended treatments.

21. When Plaintiff and Class Members viewed pages on Defendant's Website, including those related to mental health conditions, Defendant transmitted this information to Meta.

22. Defendant's transmission of information to Meta included the specific pages viewed by consumers, as well as the consumer's FID which is a string of numbers unique to each Facebook profile that personally identifies the member.

23. Anyone who possesses a FID may use this number to quickly and easily locate, access, and view the corresponding Facebook profile by simply visiting www.facebook.com/[the user's FID]. Facebook profiles contain large amounts of personal information.

24. A Facebook profile typically shows the Facebook user's name, gender, place of residence, career, educational history, a multitude of photos, and the content of the user's posts. This information may reveal even more sensitive personal information—for instance, posted photos may disclose the identity of family members, and written posts may disclose religious preferences, political affiliations, personal interests and more.

25. Just as Meta can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of a FID. Thus, equipped with a FID and the URL of the pages that were viewed on

Defendant's Website, any ordinary person could determine the identity of the Website visitor and the specific mental health conditions they viewed on Defendant's Website.

26. Defendant transmits the FID and pages visited to Meta in a single transmission, through a Meta Pixel. A Meta Pixel is a snippet of a programming code that, once installed on a webpage, sends information to Meta. This transmission occurs when a member views a page on Defendant's website.

27. The Meta Pixel is an advertising tool that allows website owners to track visitor actions on their websites for purposes of sending the corresponding information to Meta; websites use the Pixel in hopes of better targeting their products and services on Facebook to interested consumers. Thus, a business such as Defendant chooses to install the Pixel on its website in order to increase its profits.

28. According to Meta's website, the Meta Pixel allows it "to match your website visitors to their respective Facebook User accounts" and that "[o]nce matched, we can tally their actions in the Facebook Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."[1]

29. Defendant knew that by installing the Meta Pixel on its Website, the Pixel would send Meta information identifying Website visitors and the pages they visited.

30. Meta's website explains that, to begin using the Meta Pixel, a business must first "install" the Pixel "by placing the Meta Pixel base code on all pages of your website."[2] Defendant made the conscious decision to undertake this installation process.

31. Meta benefits from websites like Defendant's installing its Pixel. When the Pixel is installed on a business's website, the business has a greater incentive to

---

[1] https://developers.facebook.com/docs/meta-pixel/get-started (last visited March 13, 2025).

[2] Id.; https://www.facebook.com/business/tools/meta-pixel/get-started (last visited March 13, 2025).

advertise through Facebook or other Meta owned platforms, like Instagram. In addition, even if the business does not advertise with Facebook, the Pixel assists Meta in building more fulsome profiles of its own users, which in turn allows Meta to profit from providing more targeted ads. The Pixel is installed on a variety of websites and, accordingly, provides Meta with information about its users' preferences, other distinguishing traits, and web browsing activities outside of Meta-owned platforms.

32. Using the Meta Pixel likewise benefits Defendant's business by improving its ability to promote its content and services, thereby increasing its profits.

33. Through use of the Meta Pixel, Defendant discloses to Meta the pages a person visited, together with the person's FID, thus linking members' mental health conditions to their Facebook profiles.

34. Defendant violates and invades the privacy rights of consumers with its practice of sending their FIDs, together with their viewing content, to Meta. Plaintiff and Class Members did not know of or consent to Defendant's disclosure of their Private Information to Meta.

35. At no point was Plaintiff or any other Website visitor asked for consent to such sharing. Hence, no individual consented to Defendant's offending practice of sharing Private Information with third parties.

36. Defendant shared with Meta the Private Information of Plaintiff and Class Members, including their mental health conditions, which they reasonably expected would be kept private.

37. Plaintiff and Class Members used Defendant's Website, and not another competitor's website, because they trusted that Defendant's privacy practices comported with their privacy preferences.

38. Defendant's practice of sharing consumers' Private Information with Meta without their consent, and its failure to disclose this practice, caused Defendant to profit from advertising revenue it would otherwise not have received.

How A Medical Website Like Defendant's Transmits Confidential Medical Information Through GET And POST Requests

39. A GET request is an HTTP method used by a web browser or application to retrieve specific information from a server. It is commonly employed when a consumer enters a search term, navigates to a particular page, or interacts with a website's interface.

40. The purpose of a GET request is to send a request to the server, which then returns the requested resource, such as a webpage or data. Importantly, the data sent via a GET request is appended to the URL in plain text, making it inherently unencrypted and visible in the browser's address bar.

41. Because GET requests transmit data in the open through the URL, any private information included, such as search terms, can be exposed. For example, when a consumer searches for medical symptoms or conditions on a website, those search terms can become part of the visible URL.

42. This means that any third parties monitoring the connection, including advertisers or analytics companies, can potentially intercept and record this information. The inclusion of such sensitive data in GET requests creates a significant privacy risk, particularly when dealing with medical or other confidential information.

43. Additionally, GET requests can simultaneously transmit data to third-party websites without the consumer's knowledge or consent. Through the use of tracking scripts and embedded links, a website can forward the URL, including the GET request data, to third-party entities such as advertising networks or analytics providers.

44. These third parties, like Meta, can then collect, store, and process this sensitive information for their own purposes, effectively spying on the consumer's browsing activity.

45. A POST request, by contrast, is an HTTP method used to send larger amounts of data from the consumer to a server, often as part of form submissions or account interactions.

46. POST requests are designed to transmit data in the body of the HTTP request rather than in the URL, which can offer better protection for sensitive information.

47. However, POST requests are not inherently encrypted, meaning that without the use of secure protocols such as HTTPS, the data transmitted via POST requests remains vulnerable to interception by third parties.

48. In the context of websites that deal with sensitive consumer information, such as healthcare or financial platforms, POST requests can carry private data including names, email addresses, medical history, or even insurance information. This information, if unencrypted, can be intercepted and accessed by unauthorized parties, leading to breaches of confidentiality and consumer trust.

49. Furthermore, POST requests can also be configured to forward this sensitive data to third-party entities, often without the consumer's awareness or informed consent.

50. The unauthorized use of POST requests to transmit private medical data to third parties is particularly egregious in the context of consumer privacy rights.

51. When a consumer enters sensitive health information on a website, they reasonably expect that this data will be handled confidentially and used only for its intended purpose. However, many websites utilize embedded tracking codes that surreptitiously forward this information simultaneously, instantaneously, and in realtime to third-party analytics or advertising companies.

52. These practices expose consumers to potential harm, including discrimination, identity theft, or unauthorized profiling.

53. Both GET and POST requests, when misused, create a scenario where the consumer's private data is transmitted in the open and shared without consent.

54. Websites that fail to implement adequate safeguards or notify consumers about these practices undermine consumer trust and violate their privacy rights.

55. The unencrypted transmission of search terms, medical data, or other personal information through these HTTP methods constitutes a significant breach of confidentiality, especially when such data is shared with or accessible by third-party entities.

56. In the digital age, where consumers increasingly rely on websites to access critical information and services, the integrity and confidentiality of their interactions must be protected.

57. The misuse of GET and POST requests to disclose or transmit private consumer data, particularly sensitive medical information, without explicit consent or transparency, violates fundamental principles of data privacy and consumer protection.

58. Such actions represent a grave breach of trust and privacy, as the transmitted data included sensitive and personal medical information that should have been safeguarded by Defendant.

59. Defendant facilitated the unauthorized disclosure of individually identifiable medical information, causing harm to Plaintiff and other Class Members.

How Defendant Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted with Intercepting Communications

60. Plaintiff and other Class Members access the Website to search for information about personal mental health conditions that they may have.

61. Unbeknownst to Plaintiff and Class Members, Meta was tracking their activity the moment they entered the Defendant's Website.

62. Defendant embedded the Meta Pixel on the Website, which allowed Meta to intercept and record "click" events when Plaintiff and Class Members clicked through to various pages. Click events detail information about which page on the Website the person was viewing as well as the selections and search terms they were using.

63. Meta intercepts information including the specific mental health condition they were searching for along with a whole host of other personally,

identifying information, transmitted, instantaneously to Meta, in order to uniquely identify the user and the device accessing Defendant's website.

64. By installing the Meta Pixel on the Website, Defendant assisted Meta with intercepting visitors' confidential information related to their medical needs in order to monetize that data for targeted advertising and other purposes.

65. These interceptions also included a variety of personally identifying information which Meta then utilized to identify its account holders for targeted advertising.

66. Meta used the sensitive medical information it intercepted in real time and while in transit from Defendant's Website into its marketing tools to fuel its targeted advertising service.

67. Plaintiff never consented, agreed, authorized, or otherwise permitted Meta to intercept her confidential health information.

68. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to share her confidential health information with Meta.

69. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications.

70. Defendant deprived Plaintiff of her privacy rights when it implemented a system that surreptitiously tracked and recorded Plaintiff's and other online consumers' confidential communications, personally identifiable information, and protected health information.

Warning on Tracking Codes on Health Care Websites

71. The federal government has issued guidance warning that tracking codes like the Meta Pixel may violate federal privacy law when installed on healthcare websites such as Defendant's.

72. The statement titled, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (the "Bulletin"), was issued by the Department of Health and Human Services' Office for Civil Rights

("OCR") in December 2022[3].

73. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as the Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***

The bulletin then further discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI***. Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.***
>
> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI***

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed March 13, 2025).

> ***only as expressly permitted or required by the HIPAA Privacy Rule.***
>
> Id. (footnotes omitted; bold italics added).

74. Plaintiff and Class Members face the very same kinds of risks that the government describes concerns about in this bulletin

75. Defendant disclosed the sensitive pages that Plaintiff and Class Members visited on the Website and then immediately broadcast those in real time and simultaneously to Meta.

76. This information is, as described by the OCR in its bulletin, "highly sensitive."

77. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.
>
> Id. (footnotes omitted; bold italics added).

78. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or***

payment for care.

Id. (footnotes omitted; bold italics added).

79. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."
>
> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These

> tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.
>
> . . . Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC's Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule . . .[4]

80. Defendant's conduct with respect to its Website data sharing practices is directly contrary to clear pronouncements by the FTC and HHS.

B. Plaintiff's Allegations

81. On or about September 15, 2024, Plaintiff visited the Website. Defendant shared her Private Information with Meta.

82. Plaintiff values her privacy while web-browsing especially regarding mental health.

[4] https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking (last accessed March 13, 2025)

83. The pages Plaintiff visited constitute personal information of a private and confidential nature and are assets to which no third party has a presumptive right to access.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class defined as all natural persons in the United States who, during the Class Period, visited the Defendant's Website (the "Class").

85. Plaintiff also brings this action on behalf of a subclass defined as all natural persons in California who, during the Class Period, visited the Website (the "California Subclass") (together with the Class, the "Classes").

86. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

87. The "Class Period" is the time beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment.

88. Excluded from the Classes are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer, director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his/her spouse and immediate family members; and members of the judge's staff.

89. **Numerosity**. Members of the Classes are so numerous that joinder of all members is impracticable. The exact number of Class Members is unknown to Plaintiff at this time; however, it is estimated that there are at least thousands of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records.

90. **Typicality**. Plaintiff's claims are typical of the claims of the Classes because Plaintiff used the Website to research and review sensitive mental health

conditions and had her personally identifiable information and protected health information disclosed to Meta without her express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

91. **Adequacy**. Plaintiff is prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation, generally, and in the emerging field of digital privacy litigation, specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

92. **Commonality and Predominance**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

a. Whether Defendant intentionally tapped the lines of internet communication between visitors to the Website and Defendant;

b. Whether the Website surreptitiously recorded personally identifiable information, protected health information, and related communications and subsequently, or simultaneously, disclosed that information to Meta;

c. Whether Meta is a third-party eavesdropper;

d. Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;

e. Whether Defendant's conduct, which allowed Meta—unauthorized persons— to view Plaintiff's and Class Members' personally identifiable information and protected health information, resulted in a breach of

confidentiality;

f. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using the Meta Pixel to record and communicate their confidential medical communications;

g. Whether Plaintiff and Class Members are entitled to damages under the ECPA, CIPA, or any other relevant statute; and

h. Whether Defendant's actions violated Plaintiff's and Class Members' privacy rights.

93. **Superiority**. Class action treatment is the superior method for the fair and efficient adjudication of this controversy. Such treatment permits a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweigh any potential difficulties in the management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I

Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)

94. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Nationwide Class.

95. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511. The ECPA protects both sending and the receipt of communications.

96. 18 U.S.C. § 2520(a) provides a private right of action to any person

whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

97. The transmission of Plaintiff's private and confidential information to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

98. The transmission of the private and confidential information between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

99. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

100. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

101. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

102. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Meta used to track Plaintiff's and Class Members' communications while they were navigating the Website;
b. Plaintiff's and Class Members' browsers;
c. Plaintiff's and Class Members' mobile devices;
d. Defendant's and Meta's web and ad servers;

e. The plans Defendant and Meta carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

103. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

104. By utilizing and embedding the Meta Pixel on its Website, Defendant intentionally intercepted in real time and while in transit, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

105. Specifically, Defendant intercepted in real time and while in transit Plaintiff's and Class Members' electronic communications through the Meta Pixel's software implementations on its website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' private and confidential information to third parties, such as Meta.

106. Defendant intercepted in real time and while in transit or assisted in the interception of communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding private and confidential information, including their Meta account and mental health conditions. This confidential information was then monetized for targeted advertising purposes.

107. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to Meta, their affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

108. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. §

2511(1)(d).

109. Defendant intentionally intercepted in real time and while in transit or intentionally assisted in the interception of the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

110. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual,
> that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 .S.C. § 1320d-6.

111. Plaintiff's information that Defendant assisted Meta in intercepting qualifies as IIHI, and Defendant violated Plaintiff's and Class Members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Meta

Pixel to track and utilize Plaintiff's and Class Members' private and confidential information for financial gain.

112. Defendant was not acting under the color of law to intercept Plaintiff's and Class Members' wire or electronic communications.

113. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy through the Meta Pixel.

114. Plaintiff and Class Members had a reasonable expectation that Defendant would not intercept or assist in the interception of their private and confidential information without their knowledge or consent.

115. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

116. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, *et seq.* under 18 U.S.C. § 2520.

COUNT II

Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631

117. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the California Subclass.

118. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code sections 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications " Cal. Penal Code § 630.

119. A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in

> any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .
>
> Cal. Penal Code § 631(a).

120. Further, a person violates Section 631(a) if s/he "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned" in the preceding paragraph. *Id.*

121. To avoid liability under Section 631(a), a defendant must show it had the consent of **all** parties to a communication.

122. At all relevant times, Defendant aided, agreed with, and conspired with Meta to track and intercept Plaintiff's and Class Members' internet communications while accessing the Website. These communications were intercepted in real time and while in transit without the authorization and consent of Plaintiff and Class Members.

123. Defendant, when aiding and assisting Meta's wiretapping and eavesdropping, intended to help them learn some meaning of the content in the URLs, the specific search terms typed in by the website's visitor, and the content the visitor requested.

124. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Meta Pixel falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Meta used to track Plaintiff's and Class

Members' communications while they were navigating the Website

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Meta's web and ad servers;

e. The web and ad-servers from which Meta tracked and intercepted in real time and while in transit Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by Meta to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and

g. The plans Meta carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile device to visit the Website.

125. The information that Defendant transmitted using the Meta Pixel constituted sensitive and confidential personally identifiable information.

126. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its website visitors' sensitive and confidential online communications through the Website without their consent.

127. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages. Additionally, California Penal Code section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

128. Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT III

Invasion of Privacy Under California's Constitution

129. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

130. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential online communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

131. At all relevant times, by using the Meta Pixel to record and communicate Website visitors' sensitive and confidential online medical communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

132. Plaintiff and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, health information, and other data would remain confidential, and that Defendant would not install wiretaps on the Website.

133. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable health information to Meta.

134. This invasion of privacy was serious in nature, scope, and impact because it related to individuals' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

135. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

COUNT IV

Violation of the California Computer Data Access and Fraud Act

Cal. Penal Code. § 502

136. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

137. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The enactment of the CDAFA was motivated by the finding that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . unauthorized access to computers, computer systems, and computer data." *Id.*

138. Plaintiff's and Class Members' mobile computing devices and personal computers constitute "computers" within the scope of the CDAFA.

139. Defendant violated the CDAFA Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

140. Defendant violated the CDAFA Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

141. Defendant violated the CDAFA Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

142. Defendant knowingly accessed Plaintiff's and Class Members' computers without their permission by including within the third-party Meta Pixel described herein, which intercepts and transmits data, communications, and personal information concerning Plaintiff and Class Members.

143. Defendant used data, communications, and personal information that it intercepted in real time and while in transit and took from Plaintiff's and Class Members' computers to wrongfully and unjustly enrich itself at the expense of Plaintiff and Class Members.

144. Defendant took, copied, intercepted in real time and while in transit, and made use of data, communications, and personal information from Plaintiff's and Class Members' computers.

145. Defendant knowingly and without Plaintiff's and Class Members' permission accessed or caused to be accessed their computers, by installing its Meta Pixel without Plaintiff's and Class Members' informed consent, a software that intercepts and/or takes data, communications, and personal information concerning Plaintiff and Class Members.

146. Plaintiff and Class Members are residents of California and used their computers in California at all relevant times in which Defendant made such unauthorized access.

147. Defendant accessed or caused to be accessed Plaintiff's and Class Members' data, communications, and personal information from California.

148. Defendant uses data servers that are in part located in California and allow Defendant to access and process the data, communications and personal information concerning Plaintiff and Class Members.

149. Defendant was unjustly enriched by intercepting, acquiring, taking, or using Plaintiff's and Class Members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

150. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiff and Class Members suffered damages.

151. Pursuant to CDAFA Section 502(e)(1), Plaintiff and Class Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

152. Pursuant to CDAFA Section 502(e)(2), Plaintiff and Class Members seek an award of reasonable attorneys' fees and costs.

153. Pursuant to CDAFA Section 502(e)(4), Plaintiff and Class Members seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.

COUNT V

Use of a Pen Register or Trap and Trace Device

Cal. Penal Code § 638.51

154. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed California Subclass.

155. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

156. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

157. Defendant's third-party software from Meta installed on Plaintiff's and other Class Members' devices by its Website constitutes a "pen register" because it is a device or process that records addressing or signaling information—Plaintiff's and Class Members' location data and other sensitive personal information—from the electronic communications transmitted by their computers.

158. Defendant was not authorized by any court order to use a pen register to track Plaintiff's and Class Members' location data and personal information.

159. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered losses and were damaged in an amount to be determined at trial.

COUNT VI

Violation of the Computer Fraud and Abuse Act

18 U.S.C. § 1030

160. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class.

161. Plaintiff alleges that Defendant violated the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing Plaintiff's and Class Members' devices without authorization, or by exceeding authorized access, to obtain information from protected computers used in interstate or foreign commerce.

162. Plaintiff's device qualifies as "protected computers" under the CFAA, as it is connected to the internet and used in interstate communications.

163. Plaintiff further alleges that Defendant intentionally accessed Plaintiff's and Class Members' protected computers to obtain private and sensitive information, including but not limited to geolocation data, search histories, keystrokes, communications, and page viewing activities, without authorization or consent, in violation of 18 U.S.C. § 1030(a)(2).

164. As a direct and proximate result of Defendant's unauthorized access, Plaintiff and Class Members suffered loss and damage, including the invasion of their privacy and the unauthorized use of their personal information. Plaintiff alleges that Defendant's violations of the CFAA entitle her to recover compensatory damages and injunctive relief under 18 U.S.C. § 1030(g).

165. The statute provides that any person suffering damage or loss due to a violation may maintain a civil action to obtain compensatory damages, injunctive relief, or other equitable relief.

166. Plaintiff alleges that Defendant's actions caused "loss" as defined by 18 U.S.C. § 1030(e)(11), which includes the impairment of the integrity and availability of data, programs, and systems on Plaintiff's and Class Members' protected computers.

167. As a result of Defendant's conduct, Plaintiff and Class Members are entitled to recover damages in an amount to be proven at trial, including statutory damages for any damage or loss caused by Defendant's unauthorized access.

COUNT VII

Violation of the Stored Communications Act

18 U.S.C. § 2701

168. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class.

169. Plaintiff also alleges that Defendant violated the Stored Communications Act (SCA), 18 U.S.C. § 2701(a), by intentionally accessing Plaintiff's and Class Members' electronic communications stored on their devices without authorization.

170. Defendant accessed and obtained stored electronic communications, including search history, messages, and other data, without proper consent.

171. Plaintiff further alleges that Defendant exceeded any authorized access by using its spyware software from Meta to access and disclose Plaintiff's and Class Members' stored electronic communications for commercial gain, in violation of 18 U.S.C. § 2701(a)(1) and (a)(2).

172. As a result of Defendant's violations of the Stored Communications Act, Plaintiff and Class Members are entitled to statutory damages of no less than $1,000 per violation under 18 U.S.C. § 2707(c).

173. Additionally, Plaintiff and Class Members are entitled to recover punitive damages under the SCA if it is established that Defendant acted with willful or intentional disregard for the privacy rights of Plaintiff and Class Members.

174. Plaintiff seeks compensatory damages, statutory damages, punitive

damages (as applicable), and injunctive relief for Defendant's violations of both the CFAA and the SCA, along with reasonable attorneys' fees and costs as provided under 18 U.S.C. §§ 1030(g) and 2707(b), respectively.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

a) For a determination that this action is a proper class action;

b) For an order certifying the Classes, naming Plaintiff as representative of the Classes, and naming Plaintiff's attorneys as Class Counsel to represent the Classes;

c) For an order declaring that Defendant's conduct violates the statutes referenced herein;

d) For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

e) An award of statutory damages to the extent available;

f) For punitive damages, as warranted, in an amount to be determined at trial;

g) For prejudgment interest on all amounts awarded;

h) For injunctive relief as pleaded or as the Court may deem proper; and

i) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiffs and Class Members are entitled to, and demand, a trial by jury.

Respectfully submitted,

Swigart Law Group

Date: March 27, 2025

By: *s/ Joshua Swigart*
Joshua B. Swigart, Esq.
Josh@SwigartLawGroup.com

Ben Travis
ben@bentravislaw.com
Ben Travis Law, APC
4660 La Jolla Village Drive, Suite 100
San Diego, CA 92122
Phone: (619) 353-7966

Attorneys for Plaintiff
and the Putative Class